ซอฟต์แวร์

ยืน ภู่วรวรรณ

ลับสมอง ประลองปัญญา : พิชิตไวรัสด้วยโปรแกรมสแกน

แข่งกันสร้าง แข่งกันคิด
เพื่อพิชิตไวรัสคอมพิวเตอร์
พร้อมประกาศรายชื่อผู้รับรางวัล
คำถามฉบับที่ 89

ลับสมองประลองปัญญาฉบับนี้ ผู้เขียนขอให้ลองสร้างโปรแกรมที่เป็นประโยชน์ต่อวงการ เพื่อพิชิตไวรัสด้วยการตรวจสอบไวรัสด้วยลายเซ็น (signature)

ก่อนอื่นมาทำความเข้าใจโครงสร้างของ Signature ของไวรัส ซึ่งก็คือรูปแบบสตริงที่เป็นเลขฐานสิบหกจำนวนหนึ่ง ตัวอักขระที่ปรากฏในสตริงนี้ จะเป็นรหัสแอสกีหรือไม่ก็ได้ เป็นรหัสที่อยู่ในช่วง 00-FF (ตัวเลขฐานสิบหก)

ดังนั้น Signature ก็คือ รหัสที่อยู่ในไฟล์ที่ติดไวรัส

ปัญหาที่ท่านต้องทำ

ให้เขียนโปรแกรมสแกนเพื่อใช้ในการตรวจหาไวรัสในไฟล์ใด ๆ โดยมีขั้นตอนดังนี้

1. เขียนโปรแกรมย่อยจัดการโครงสร้างแฟ้ม Signature โดยมีข้อมูลอยู่ 3 ฟิลด์คือ
   1. ฟิลด์แรกเป็นชื่อไวรัส
   2. ฟิลด์ที่สองเป็นข้อความบอกลักษณะที่ไวรัสเกาะ
   3. ฟิลด์ที่สามเป็น signature ดังตัวอย่าง

```
Adolph Virus
COM
F8F9B912B8BE1FD933FFF5F9F8FC
;
Agiplan Virus
COM EXE
AE263A2575F9BA0042263B550175F0B6BA263A75FB75E883F900
;
Aids (Taunt) Virus
COM
2A546869732046696C6520486173204265656E20496E66656374656420427920
;
Aids II (Companion) Virus
COM EXE
5589E581EC0202BFCA050E57BF3E011E57
;
```

โดยการสมมติไวรัส Signature ขึ้นเองหลาย ๆ ตัว โดยให้มี Signature ยาวสั้นไม่เท่ากัน และบางตัวมี Signature ที่เหมือนกันในตอนต้นและต่างกันในตอนท้าย เช่น Microsoft 35 กับ Microsoft เป็นต้น จัดโครงสร้างไฟล์ที่เหมาะสำหรับการนำไปใช้ในการตรวจหาไวรัสในไฟล์อื่น ๆ ให้ได้รวดเร็วที่สุด ส่วนของ Signature เก็บเป็นเท็กซ์ไฟล์ไว้ในไฟล์ชื่อ Signa.vir เมื่อโปรแกรมอ่านแฟ้ม signa.vir จะจัดโครงสร้างข้อมูลในหน่วยความจำที่พร้อมจะนำไปตรวจสอบได้

อนึ่งการเก็บข้อมูล Signature ในไฟล์ signa.vir ให้เก็บชื่อไวรัสที่อ่านออกได้ด้วย

2. เขียนโปรแกรมหลักที่อ่านไฟล์ที่ต้องการตรวจสอบไวรัส มาตรวจสอบด้วยโครงสร้างข้อมูลที่จัดไว้ในข้อ 1 เพื่อให้การตรวจสอบเร็วที่สุดเท่าที่ทำได้และให้โปรแกรมสามารถบอกได้ว่าไฟล์นี้ติดไวรัสหรือไม่ ถ้าติด ติดไวรัสอะไรบ้าง บอกชื่อมา

3. เขียนโปรแกรมเมนูเพื่อให้ผู้ใช้สามารถเลือก

3.1 เพิ่มหรือลบ ไวรัส Signature

3.2 เริ่มต้นการสแกนหาไวรัสในไฟล์อื่นที่มีส่วนขยายเป็น .EXE และ .COM หรือ .XXX ที่กำหนด

หมายเหตุ

ความเร็วในการสแกนอยู่ที่เทคนิควิธีการจัดโครงสร้างข้อมูล ขอให้ท่านเสนอแนวความคิดของท่านเท่าที่เห็นว่าดีที่สุด โดยเขียนรายละเอียดวิธีการจัดโครงสร้างข้อมูลและวิธีการค้นหาด้วย

ข้อเตือนใจ

โปรแกรมนี้เป็นโปรแกรมที่ไม่ยาก การค้นหาสตริงในไฟล์นี้จึงเป็นเรื่องที่ทำได้ง่าย แต่ถ้ามีสตริงหลายตัวที่ต้องการค้นหาในรอบเดียว จะทำอย่างไรให้ได้ประสิทธิภาพดี ลองเปรียบเทียบความเร็วของโปรแกรมเทียบกับโปรแกรม SCAN ที่มีในท้องตลาด ดูว่าใครจะเร็วกว่ากัน

สำหรับผู้ที่ตอบในฉบับที่ 89 เรื่อง เดินเบี้ยบนกระดานสามเหลี่ยมที่ได้รับรางวัล ได้แก่

1. คุณคานธี ทองจุไร 412/5-7 สยามสแควร์ ซอย 6 กรุงเทพฯ 10330

2. คุณวิวรรธน์ ขรภูมิ 205 ถนนเมืองราษฎร์ ต.เขานิเวศน์ อ.เมือง ระนอง 85000

คุณคานธี ทองจุไร เขียนด้วยเทอร์โบซี เวอร์ชัน 2 ส่วนคุณวิวรรธน์ ขรภูมิ เขียนด้วยเทอร์โบปาสคาล ทั้งสองท่านทำได้ตรงตามข้อกำหนดทุกประการ

กติกา

1. วารสารไมโครคอมพิวเตอร์แต่ละเล่มจะเสนอปัญหา 1 ข้อ และให้ผู้อ่านใช้เวลาในการแก้ปัญหา 1 เดือน เมื่อทำเสร็จแล้วรีบส่งกลับมายังวารสารโดยด่วนครับ

2. การแก้ปัญหาโจทย์ ผู้ทำจะใช้ภาษาอะไรก็ได้ที่เป็น procedural language เช่น ปาสคาล ซี ฟอร์แทรน ฯลฯ ผู้ส่งผลงานต้องบอกด้วยว่าใช้คอมพายเลอร์อะไร เวอร์ชันไหน โดยส่งซอร์สโค้ดในรูปดิสเกตต์ และข้อความการวิเคราะห์โจทย์ตลอดจนแนวคิด

3. การแก้ปัญหานี้ผมจะมีข้อมูลสำหรับการทดสอบ ซึ่งจะยังไม่บอกไปในโจทย์แต่จะแสดงวิธีการตรวจสอบให้ในวารสารไมโครคอมพิวเตอร์ฉบับที่เฉลยปัญหา

สำหรับปัญหาในฉบับนี้ผู้สนใจลองทำดู แล้วส่งคำตอบมาที่

กองบรรณาธิการวารสารไมโครคอมพิวเตอร์

บริษัท ซีเอ็ดยูเคชั่น จำกัด

800/43-45 ซอยตระกูลสุข

ถนนอโศกดินแดง เขตห้วยขวาง

กรุงเทพฯ 10400

หมายเหตุ : ถ้าหากโปรแกรมที่ส่งมามีลักษณะซ้ำกันหรือเหมือนกันทุกประการ ทางวารสารจะพิจารณาเฉพาะโปรแกรมของท่านที่ส่งมาถึงวารสารก่อนเป็นอันดับแรก

: โปรดจ่าหน้าซองจดหมาย หรือพัสดุว่า "คอลัมน์ลับสมองประลองปัญญา"

"รีบหน่อยนะครับของสมนาคุณรอท่านอยู่แล้ว"